In re Application of: YANOVSKY
Serial No.: 10/520,274
Filed: January 18, 2005
Office Action Mailing Date: January 22, 2009

Examiner: SHAHROUZ
Group Art Unit: 2432
Attorney Docket: 29238

REMARKS

Reconsideration of the above-identified application in view of the amendments above and the remarks following is respectfully requested.

Claims 1 - 48 are in this Application. Claims 1 – 48 have been rejected under 35 U.S.C. § 103. Claims 1, 21 and 37 have been amended herewith.

35 U.S.C. § 103 Rejections

Claims 1 – 48 have been rejected for lack of inventive step.

Claims 1, 21 and 37 were amended in the previous response to stress the point that the *encryption keys* are *generated separately* at the two different parties. Examiner, as best understood by the applicant, rejected this position on the basis that Seiheidt only exchanges key derivatives so that the final key sequences are in practice generated separately at each party.

Applicant now amends the claims to define that there are two randomizers, one at each party, and both set with identical settings, so that both obtain the same derived sequence if looking at the same exchanged data, thus:

> "a random selector configured *with selection settings identical to those at said second party* for selecting, from said bitstream, *a series of bits* in accordance with a randomization *seeded by said data exchanged* between said parties, said randomization being identical to a randomization carried out at said second party, thereby ensuring that said series of bits is identical at both parties;"

Seiheidt does not teach a randomizer, as the Examiner concedes at page 3 third line from the end, of his Office Action.

Tan teaches a random selector at the encryption end – in this case Alice - however Tan fails to teach that there are two random selectors with identical settings, one at each party. More particularly, Tan does not teach that there is a random selector at the decryption end. Tan further fails to teach that the two random selectors are *to choose a series of bits* using data *exchanged* between the parties.

On the contrary, Tan in column 10 last four lines, teaches that the random number on which the encryption is based is actually *exchanged* between the parties as part of the seed. "Bob enters the pass phrase to generate the master key *from the random number retrieved from the seed*" (Tan col. 10 lines 65 – 68 – Emphasis added).

On the contrary, as described in Tan with respect to Fig. 1, encryption is carried out by Alice using a random sequence generated by her selector, and then a seed is transferred to Bob to enable him to decrypt the message. The seed contains the random number and thus no random selector is required by Bob at all. It is certainly unnecessary for identically set random selectors to choose the same bit sequences at the two parties.

The information missing in Tan – namely that there is a second identically set random selector at the decryption end, is also missing from Seiheit. Thus even if the teaching of Seiheit were to be augmented by the random selector of Tan, the skilled person would merely place the random selector at the encryption end and would understand that he is to transfer the random number in a seed. The skilled person would not infer that (s)he should have a second random selector at the decryption end.

Nevertheless, Tan suffers a fatal flaw, in that if an eavesdropper can merely pick up the seed, he has all the information he needs to decrypt the message. The present invention solves this problem in that there is no seed to intercept.

The same amendment is made to the remaining independent claims.

The dependent claims are believed to be allowable as being dependent on an allowable main claim.

In view of the above amendments and remarks it is respectfully submitted that claims 1 - 48 are now in condition for allowance. A prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Martin D. Moynihan
Registration No. 40,338

Date: May 21, 2009

Enclosure:

- [] Petition for Extension (One Month)
- [] Request for Continued Examination (RCE)